CLAIMS

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

1. System for authenticating digital information, comprising:

a) an image acquisition device for producing an original array of two-dimensional digital information;

b) means for obtaining current date and time information from satellite or radio broadcasts;

c) means for obtaining current location information from satellite or radio broadcasts;

d) means for identifying a Sensor ID for the image acquisition device;

e) an encoder for converting date/time, location, and Sensor ID into two-dimensional format called the Encoded Data Array;

f) an embedder for combining the Encoded Data Array and the Original Array into a new Composite Array

g) an encrypter for transforming the Composite Array into another two-dimensional array called the Encrypted Composite Array;

h) a Transmission Process to transfer the Encrypted Composite Array to the intended recipient;

i) a decrypter to restore the Composite Array

j) a decoder with fault indicator when date/time, location, and source cannot be decoded;

k) an Encoding Extractor for removing the Encoded Data Array from the Decrypted Composite Array;

l) means for restoring the Original Array at pixel locations used for the Encoding; and

m) means for determining changes between the Restored Original Array and the Original Array.

2. System as in Claim 1 in which the Original Array size is increased by a factor and subpixels are used in steps f through m.

3. System as in Claims 1 and 2 in which the encryption of step g and decryption of step i is repeated more than one time.

4. System as in Claims 1 and 2 in which the encryption process involves scrambling the pixels or subpixels.

5. System as in Claims 1 and 2 in which steps b and c utilize the GPS (Global Positioning Satellite) system.

6. System as in Claims 1and 2 in which the Decoder utilizes FlashCorrelation« to select pixel locations of the Encoded Data Array and test for authenticity.

7. System as in Claims 1 and 2 in which the Sensor ID in step d includes a biometric identifier of the User of the image acquisition device.

8. System as in Claims 1 and 2 in which the Sensor ID in step d includes the serial number and odometer setting of the image acquisition device of step a.

9. System as in Claims 1 and 2 in which the change detector of step m evaluates subsections of the Restored Original Array and the Original Array to localize areas of difference.

10. System as in Claim 6 in which FlashCorrelation« is used to verify that the encoded data is the same as data which is expected to be encoded into a particular Original Array.

11. System as in Claim 6 in which FlashCorrelation is used to identify the encoded data by exhaustive comparison against each possible value for each of date/time, location, and source.

12. System as in Claims 1 and 2 in which date/time, location, and source are annotated onto the Encrypted Composite Array.

13. System as in Claims 1 and 2 in which the encoded data provides the key to the encryption and decryption algorithms.

14. System of Claims 1 and 2 in which the operation of the EIS is triggered by the change of status of another device.

15. System of Claim 14 in which the triggering device is a face recognition system.

16. System of Claim 14 in which the triggering device is a speed sensor.

17. System of Claim 14 in which the triggering device is an alarm condition sensor.

18. System of Claims 1and 2 in which the Encoding is performed by overlaying a pattern of pixels of a particular color or grey scale value.

19. System of Claims 1 and 2 in which the Encoding is performed by steganography.

20. System of Claims 1 and 2 in which no encryption or scrambling is performed.

21. A method for authenticating digital images, comprising the steps of:

capturing a digital image;

recording authentication information at the time and place of said capturing, said authentication information being unique to said digital image and

including at least one piece of information from a source independent of said capturing;

encoding said authentication information into a data array mapable to said digital image;

mapping said data array to said digital image, thereby creating a composite array;

optionally encrypting said composite array;

optionally annotating said composite array;

comparing said data array, optionally encrypted and annotated, to a target composite array, wherein said comparing determines whether said authentication information is embedded in said target composite array, thereby proving that said target composite array is an authentic copy of said composite array.

22. The method of claim 21, wherein said at least one piece of information from a source independent of said capturing is GMT time information.

23. The method of claim 21, wherein said at least one piece of information from a source independent of said capturing is GPS location information.

24. The method of claim 21, wherein said at least one piece of information from a source independent of said capturing is GMT time information and GPS location information.

25. The method of claim 21, wherein said comparing step is flashcorrelation of said data array with said target composite array.

26. The method of claim 25, wherein said digital image is a sequence of digital images, there being a unique set of authenticating information for each digital image in said sequence and a corresponding unique data array, there being a unique composite array corresponding to each digital image in said sequence, wherein said composite array is a sequence of composite arrays and said target composite array is a sequence of target composite arrays, and wherein said flashcorrelation determines whether said sequence of target composite arrays is an authentic copy of said sequence of composite arrays.

27. The method of claim 26, wherein said sequence of digital images is a video image and said flashcorrelation is done in real time.

28. A system for authenticating digital images, comprising:

means for capturing a digital image;

means for recording authentication information at the time and place of said capturing, said authentication information being unique to said digital image and including at least one piece of information from a source independent of said capturing;

means for encoding said authentication information into a data array mapable to said digital image;

means for mapping said data array to said digital image, thereby creating a composite array;

means for optionally encrypting said composite array;

means for optionally annotating said composite array;

means for comparing said data array, optionally encrypted and annotated, to a target composite array, wherein said comparing determines whether said authentication information is embedded in said target composite array, thereby proving that said target composite array is an authentic copy of said composite array.

29. The system of claim 28, wherein said at least one piece of information from a source independent of said capturing is GMT time information.

30. The system of claim 28, wherein said at least one piece of information from a source independent of said capturing is GPS location information.

31. The system of claim 28, wherein said at least one piece of information from a source independent of said capturing is GMT time information and GPS location information.

32. The system of claim 28, wherein said comparing step is flashcorrelation of said data array with said target composite array.

33. The system of claim 32, wherein said digital image is a sequence of digital images, there being a unique set of authenticating information for each digital image in said sequence and a corresponding unique data array, there being a unique composite array corresponding to each digital image in said sequence, wherein said composite array is a sequence of composite arrays and said target composite array is a sequence of target composite arrays, and wherein said flashcorrelation determines whether said sequence of target composite arrays is an authentic copy of said sequence of composite arrays.

34. The system of claim 33, wherein said sequence of digital images is a video image and said flashcorrelation is done in real time.